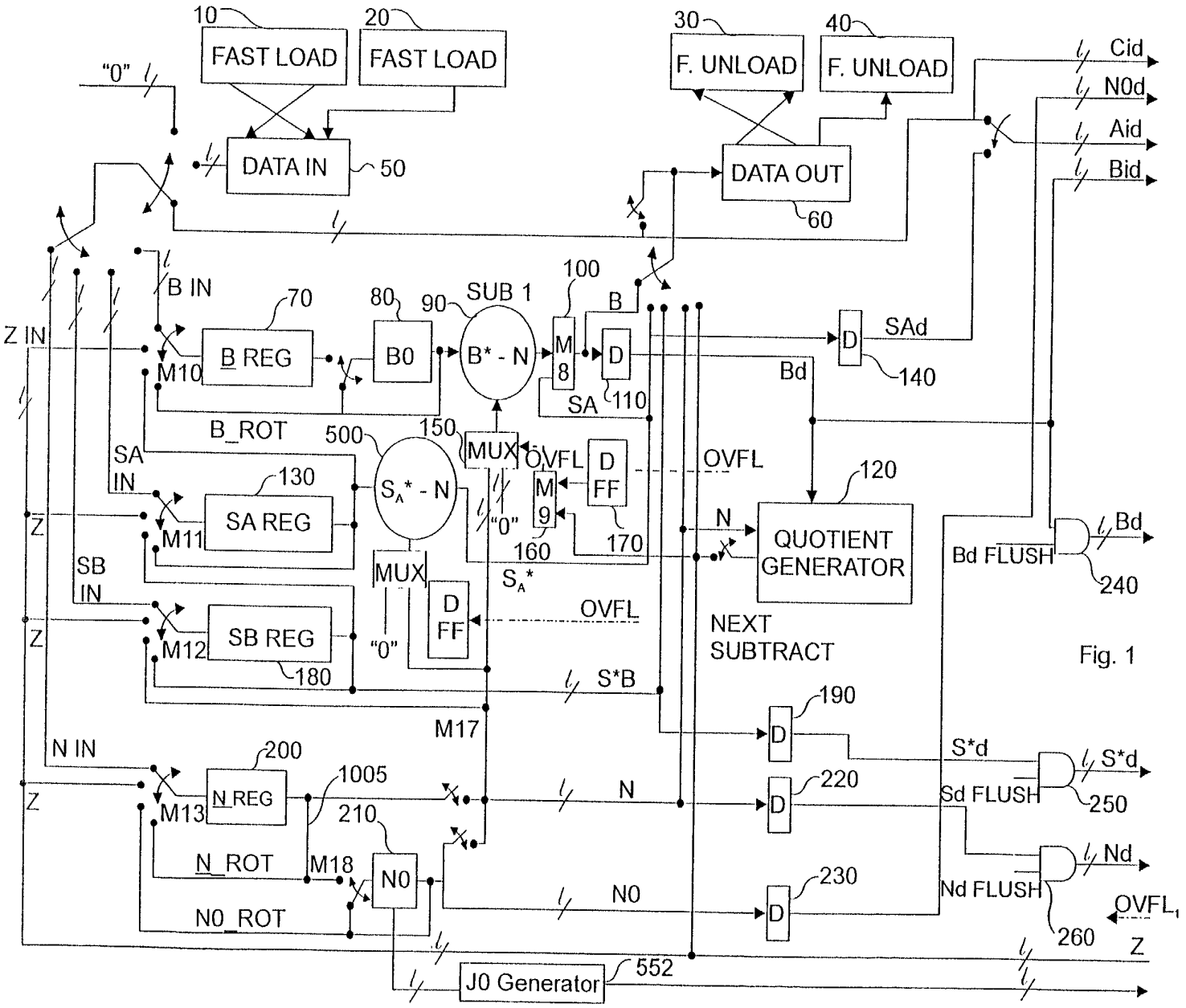

10
FAST LOAD
20
FAST LOAD
30
F. UNLOAD
40
F. UNLOAD
"0"
DATA IN
50
DATA OUT
60
Cid
N0d
Aid
Bid
B IN
Z IN
70
B REG
M10
80
B0
90
SUB 1
B* - N
100
M 8
B
D
110
SA
SAd
140
Bd
B_ROT
500
150
MUX
OVFL
D FF
OVFL
SA IN
130
SA REG
M11
S_A* - N
M 9
"0"
160
170
N
120
QUOTIENT GENERATOR
Z
SB IN
MUX
S_A*
Bd FLUSH
Bd
240
D FF
OVFL
NEXT SUBTRACT
SB REG
M12
"0"
180
S*B
Fig. 1
M17
190
N IN
200
N REG
1005
M13
N
220
S*d
Sd FLUSH
S*d
250
210
N_ROT
M18
N0
N0
230
Nd
Nd FLUSH
OVFL1
260
N0_ROT
Z
J0 Generator
552

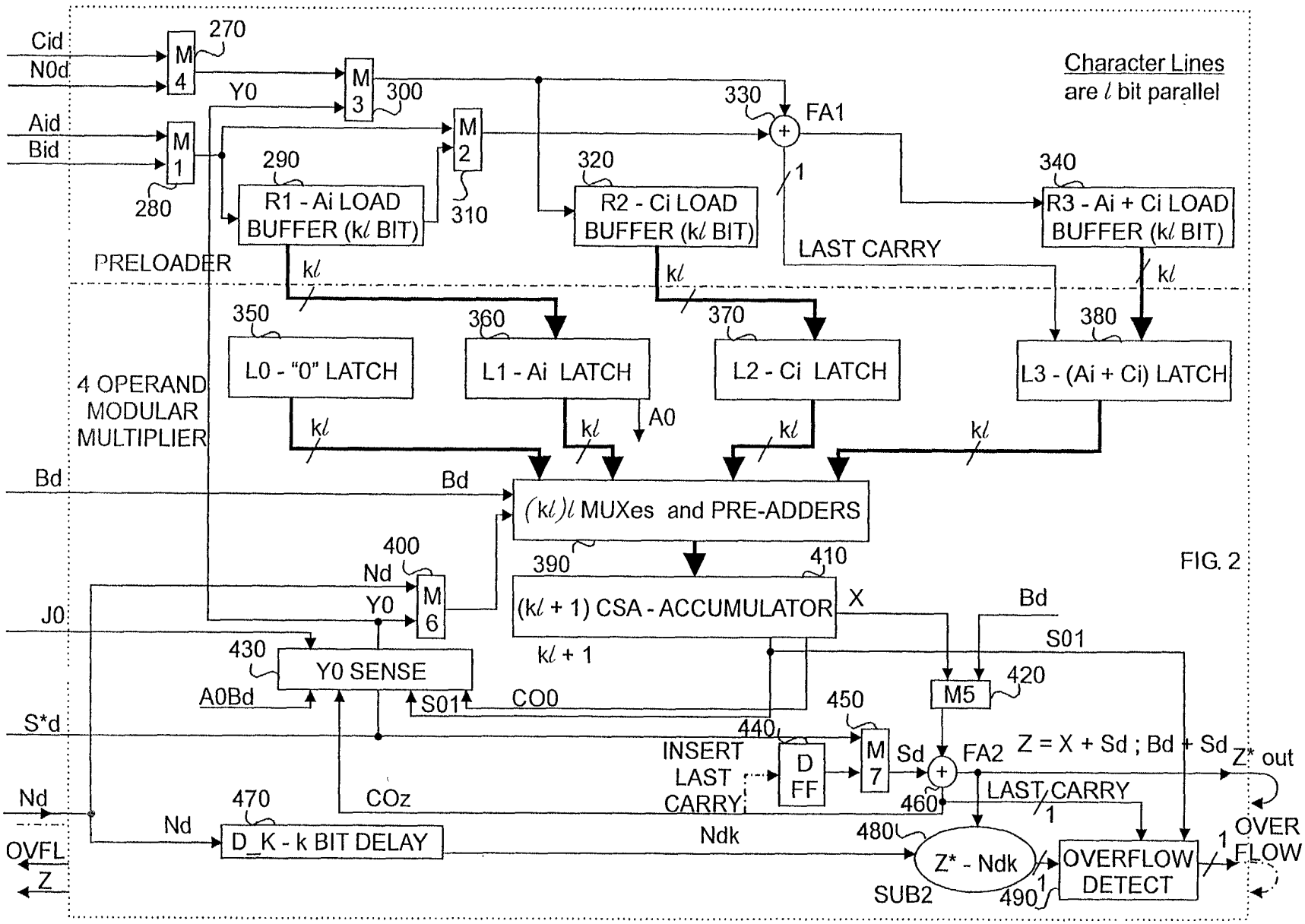

Cid
N0d
Aid
Bid
M 4
M 3
M 2
M 1
270
300
280
290
310
320
330
340
Y0
FA1
1
Character Lines
are ℓ bit parallel
R1 - Ai LOAD BUFFER (kℓ BIT)
R2 - Ci LOAD BUFFER (kℓ BIT)
R3 - Ai + Ci LOAD BUFFER (kℓ BIT)
LAST CARRY
PRELOADER
kℓ
350
360
370
380
L0 - "0" LATCH
L1 - Ai LATCH
L2 - Ci LATCH
L3 - (Ai + Ci) LATCH
A0
4 OPERAND MODULAR MULTIPLIER
Bd
(kℓ)ℓ MUXes and PRE-ADDERS
400
Nd
390
410
(kℓ + 1) CSA - ACCUMULATOR
X
M 6
J0
kℓ + 1
S01
420
M5
430
Y0 SENSE
A0Bd
S01
CO0
450
440
S*d
INSERT LAST CARRY
D FF
M 7
Sd
FA2
Z = X + Sd ; Bd + Sd
Z* out
460
LAST CARRY
Nd
470
COz
Nd
D_K - k BIT DELAY
Ndk
480
Z* - Ndk
OVERFLOW DETECT
OVER FLOW
OVFL
Z
SUB2
490

FIG. 2

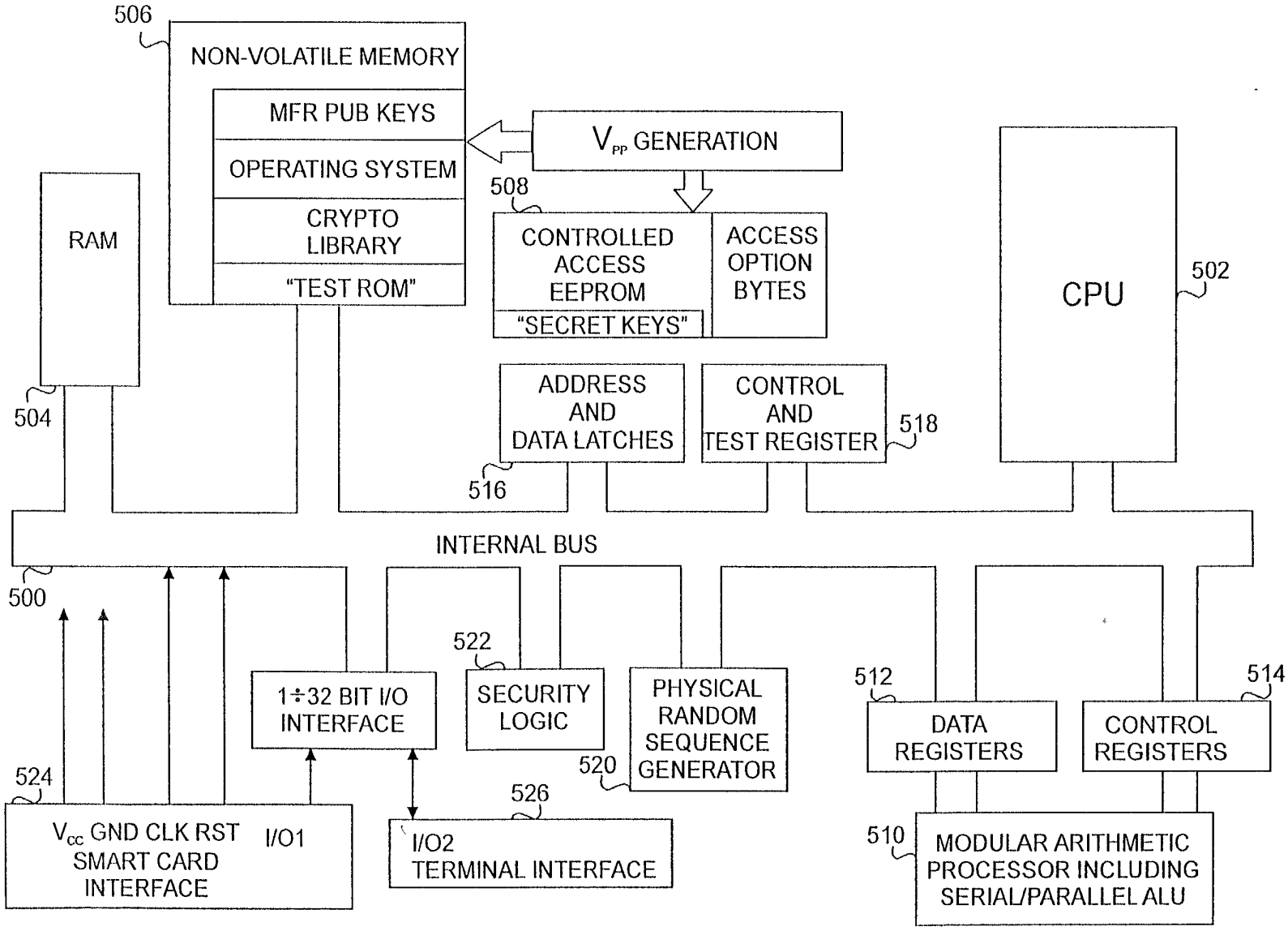

506
NON-VOLATILE MEMORY
MFR PUB KEYS
OPERATING SYSTEM
CRYPTO LIBRARY
"TEST ROM"
V_{PP} GENERATION
508
CONTROLLED ACCESS EEPROM
"SECRET KEYS"
ACCESS OPTION BYTES
RAM
504
CPU
502
ADDRESS AND DATA LATCHES
516
CONTROL AND TEST REGISTER
518
INTERNAL BUS
500
522
SECURITY LOGIC
1÷32 BIT I/O INTERFACE
PHYSICAL RANDOM SEQUENCE GENERATOR
520
512
DATA REGISTERS
514
CONTROL REGISTERS
524
V_{cc} GND CLK RST I/O1
SMART CARD INTERFACE
526
I/O2
TERMINAL INTERFACE
510
MODULAR ARITHMETIC PROCESSOR INCLUDING SERIAL/PARALLEL ALU

FIG. 3

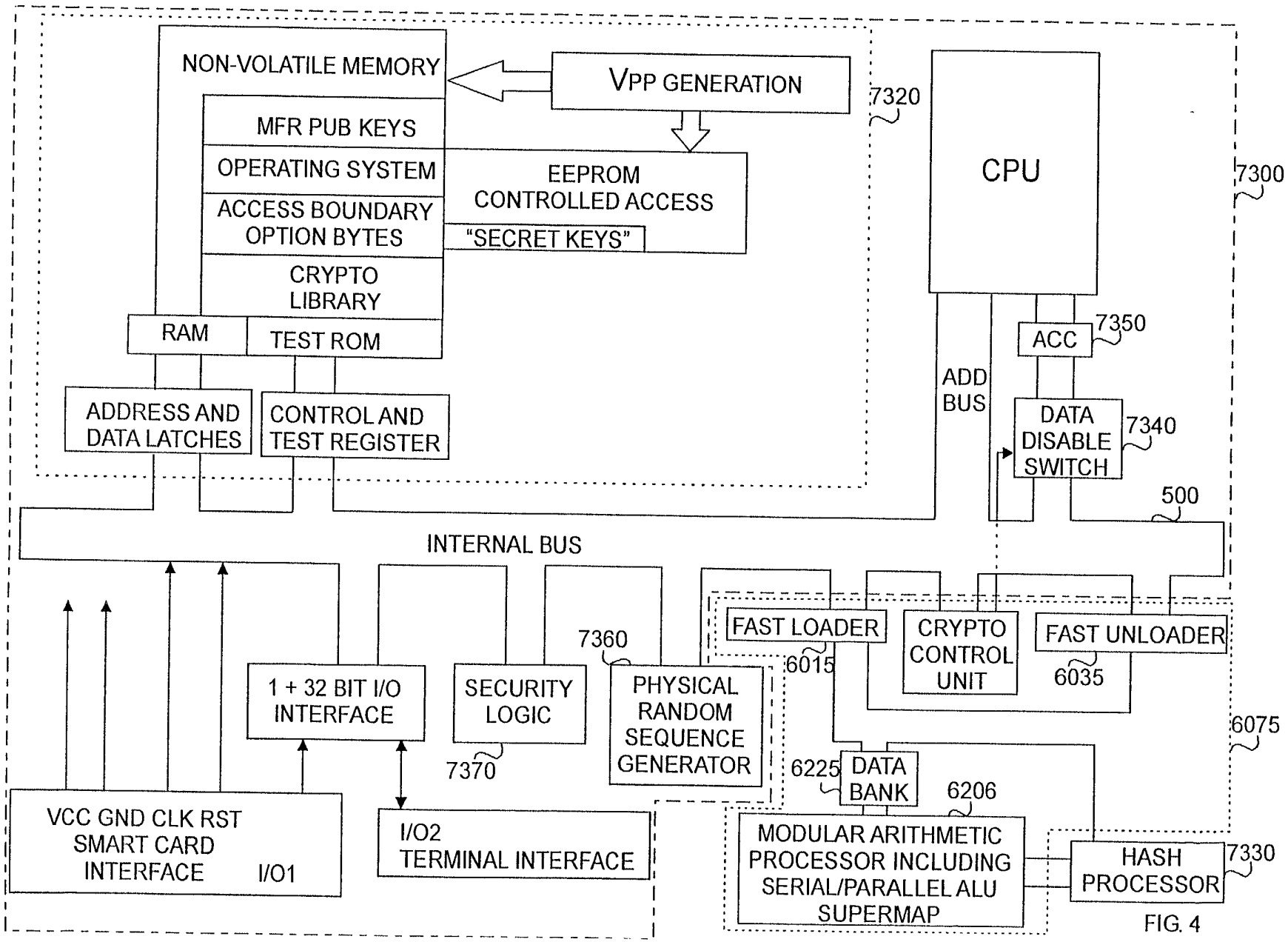

NON-VOLATILE MEMORY
VPP GENERATION
7320
MFR PUB KEYS
OPERATING SYSTEM
EEPROM CONTROLLED ACCESS
ACCESS BOUNDARY OPTION BYTES
"SECRET KEYS"
CRYPTO LIBRARY
RAM
TEST ROM
CPU
7300
ACC
7350
ADD BUS
ADDRESS AND DATA LATCHES
CONTROL AND TEST REGISTER
DATA DISABLE SWITCH
7340
500
INTERNAL BUS
FAST LOADER
6015
CRYPTO CONTROL UNIT
FAST UNLOADER
6035
7360
1 + 32 BIT I/O INTERFACE
SECURITY LOGIC
7370
PHYSICAL RANDOM SEQUENCE GENERATOR
6075
6225
DATA BANK
6206
VCC GND CLK RST SMART CARD INTERFACE I/O1
I/O2 TERMINAL INTERFACE
MODULAR ARITHMETIC PROCESSOR INCLUDING SERIAL/PARALLEL ALU SUPERMAP
HASH PROCESSOR
7330

FIG. 4

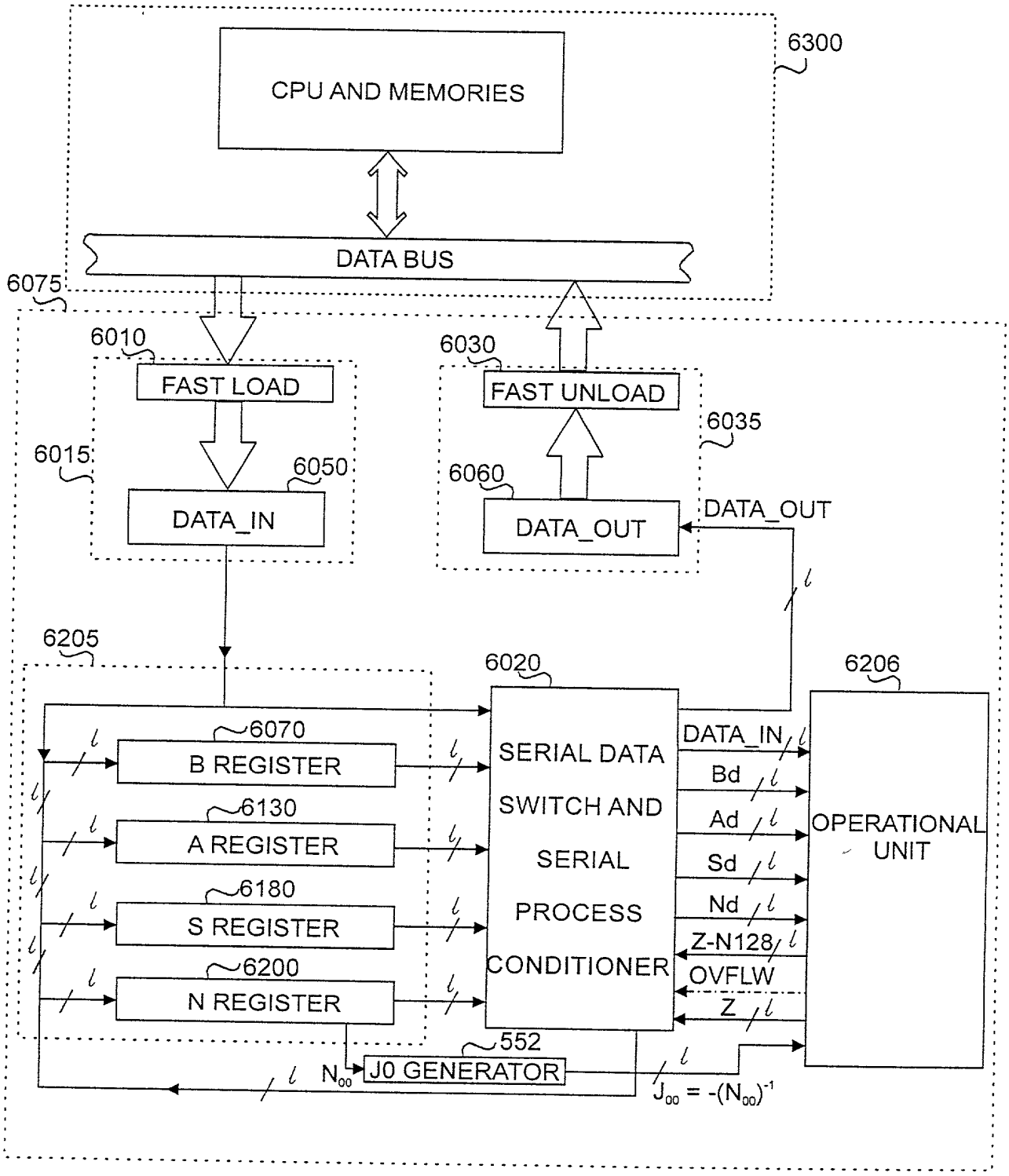

6300
CPU AND MEMORIES
DATA BUS
6075
6010
FAST LOAD
6015
6050
DATA_IN
6030
FAST UNLOAD
6035
6060
DATA_OUT
DATA_OUT
6205
6020
6206
6070
B REGISTER
6130
A REGISTER
6180
S REGISTER
6200
N REGISTER
SERIAL DATA SWITCH AND SERIAL PROCESS CONDITIONER
DATA_IN
Bd
Ad
Sd
Nd
Z-N128
OVFLW
Z
OPERATIONAL UNIT
552
J0 GENERATOR
N_{00}
$J_{00} = -(N_{00})^{-1}$

FIG. 5

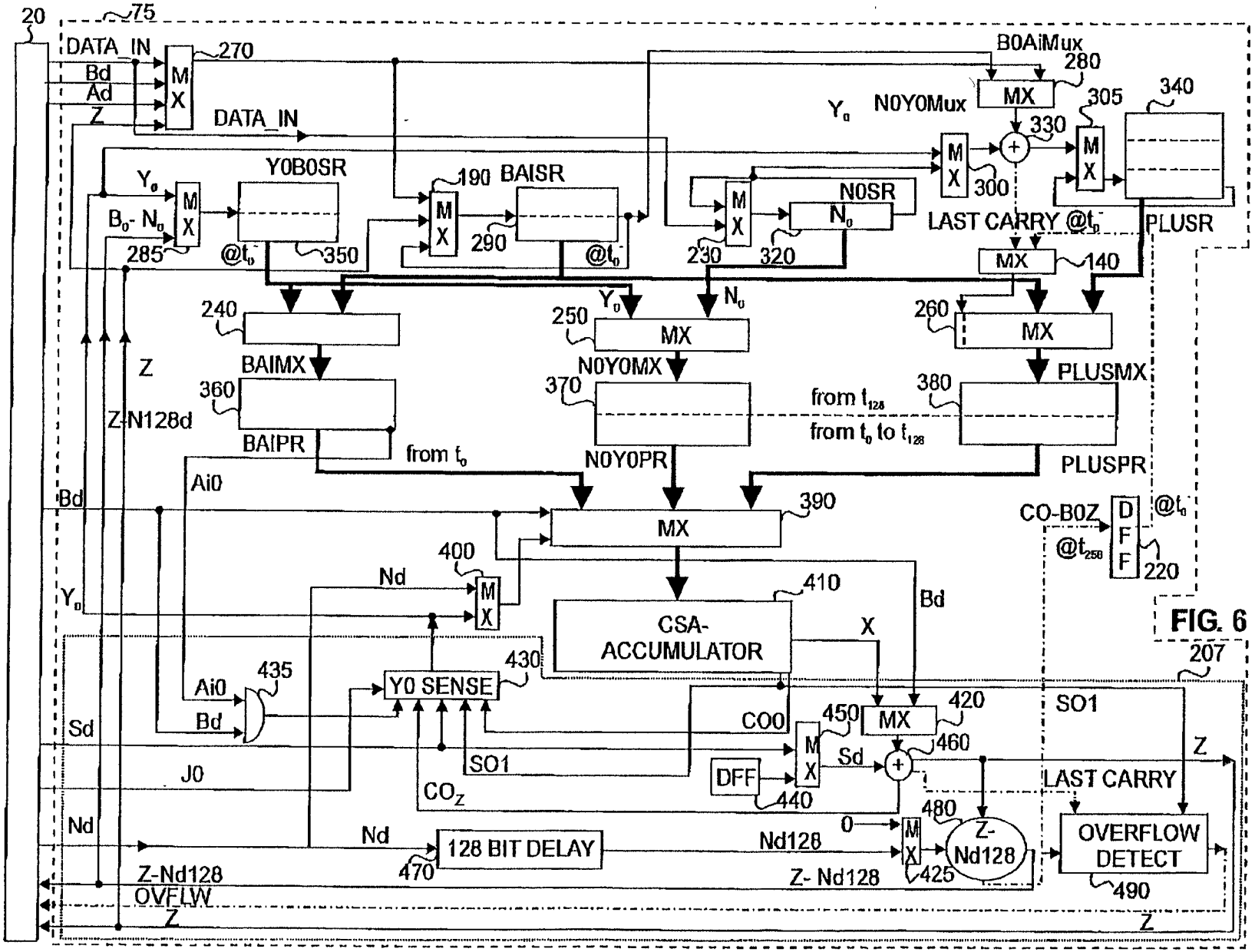


FIG. 6

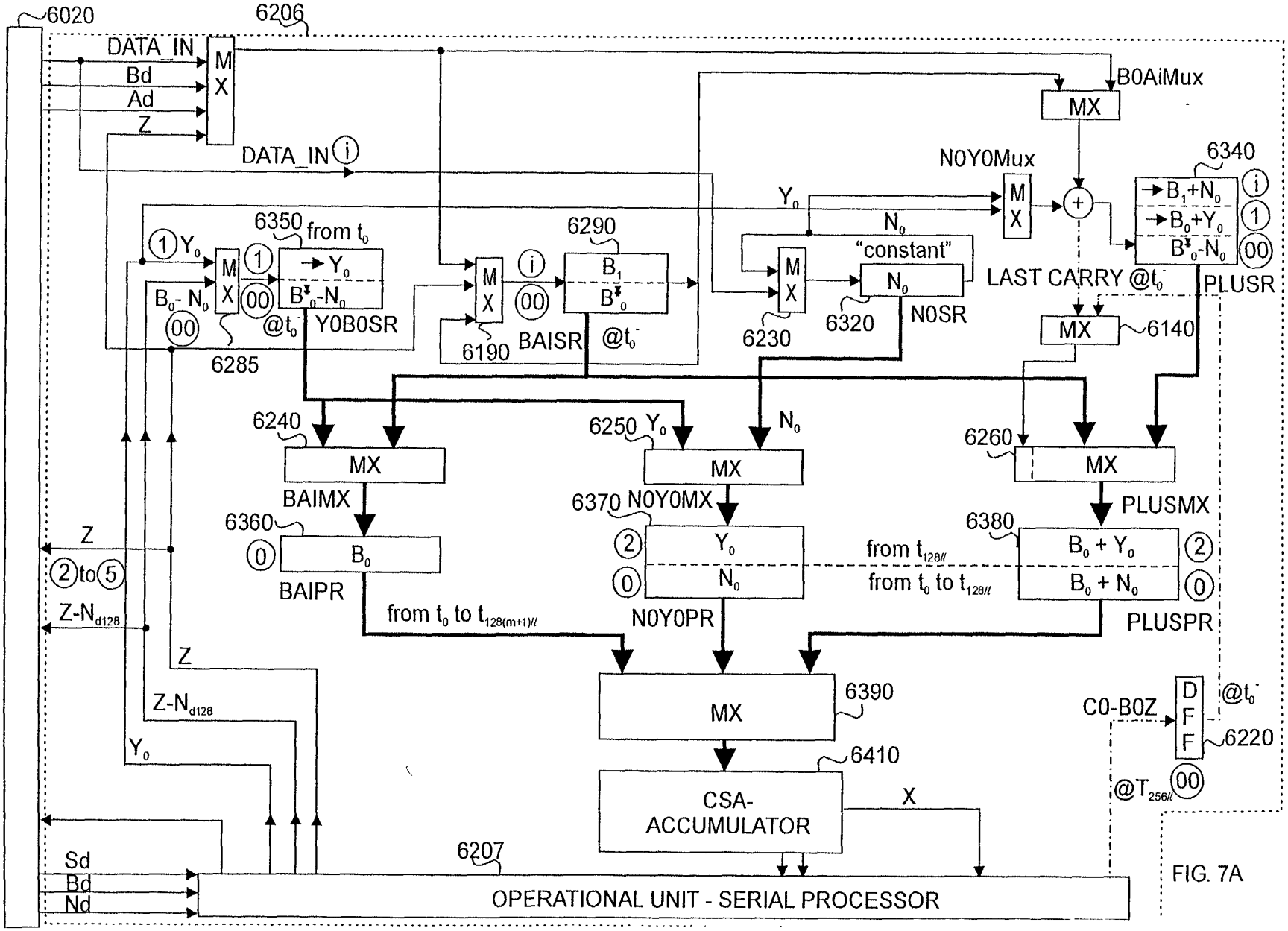

6020
6206
DATA_IN
Bd
Ad
Z
M X
DATA_IN (i)
B0AiMux
MX
N0Y0Mux
6340
B_1+N_0
B_0+Y_0
$B^{\vee}_0-N_0$
(i) (1) (00)
PLUSR
LAST CARRY @t_0^-
6350
from t_0
(1) Y_0
(1) Y_0
B_0-N_0
(00) $B^{\vee}_0-N_0$
@t_0^-
Y0B0SR
6285
6290
(i) B_1
(00) $B^{\vee}_0$
6190
BAISR
@t_0^-
Y_0
N_0
"constant"
N_0
6230
6320
N0SR
MX
6140
6240
MX
BAIMX
6250 Y_0
MX
N_0
6260
MX
PLUSMX
6360
(0) B_0
BAIPR
from t_0 to $t_{128(m+1)//}$
6370 N0Y0MX
(2) Y_0
(0) N_0
N0Y0PR
6380
B_0+Y_0
B_0+N_0
from $t_{128//}$
from t_0 to $t_{128//}$
PLUSPR
Z
(2) to (5)
$Z-N_{d128}$
Z
$Z-N_{d128}$
Y_0
MX
6390
6410
CSA-
ACCUMULATOR
X
C0-B0Z
D F F
@t_0^-
6220
@$T_{256//}$ (00)
Sd
Bd
Nd
6207
OPERATIONAL UNIT - SERIAL PROCESSOR

FIG. 7A

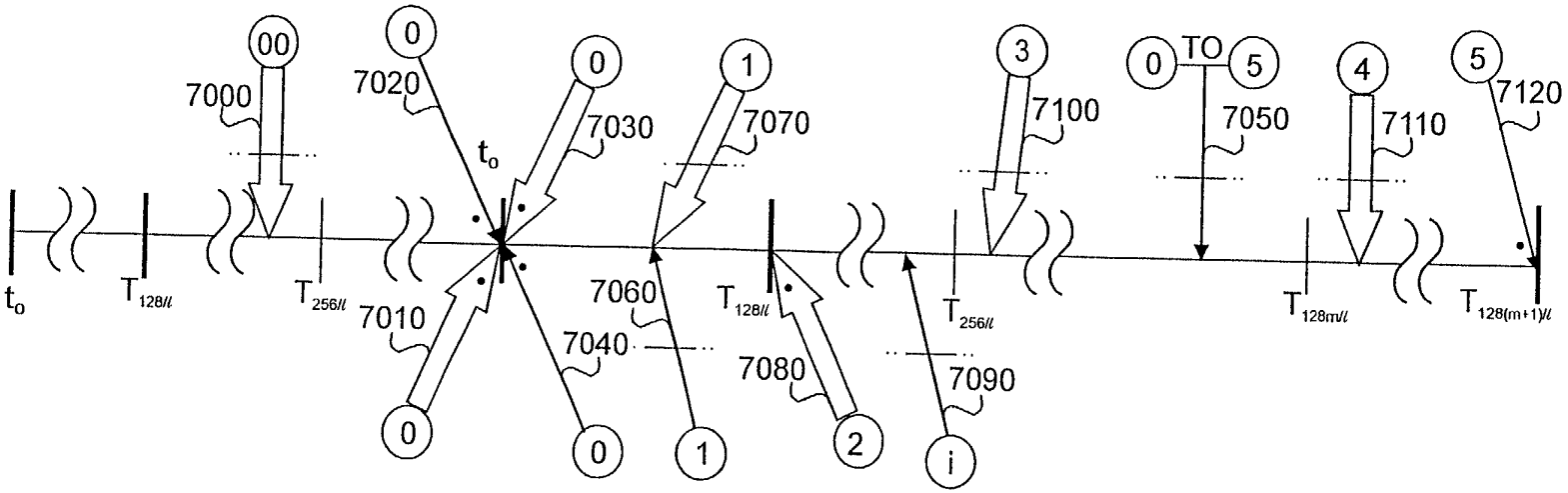

00
7000
0
7020
0
7030
1
7070
3
7100
0
TO
5
7050
4
7110
5
7120
t_o
t_o
$T_{128/\ell}$
$T_{256/\ell}$
7010
7060
$T_{128/\ell}$
7040
7080
$T_{256/\ell}$
7090
$T_{128m/\ell}$
$T_{128(m+1)/\ell}$
0
0
1
2
i

FIG. 7B

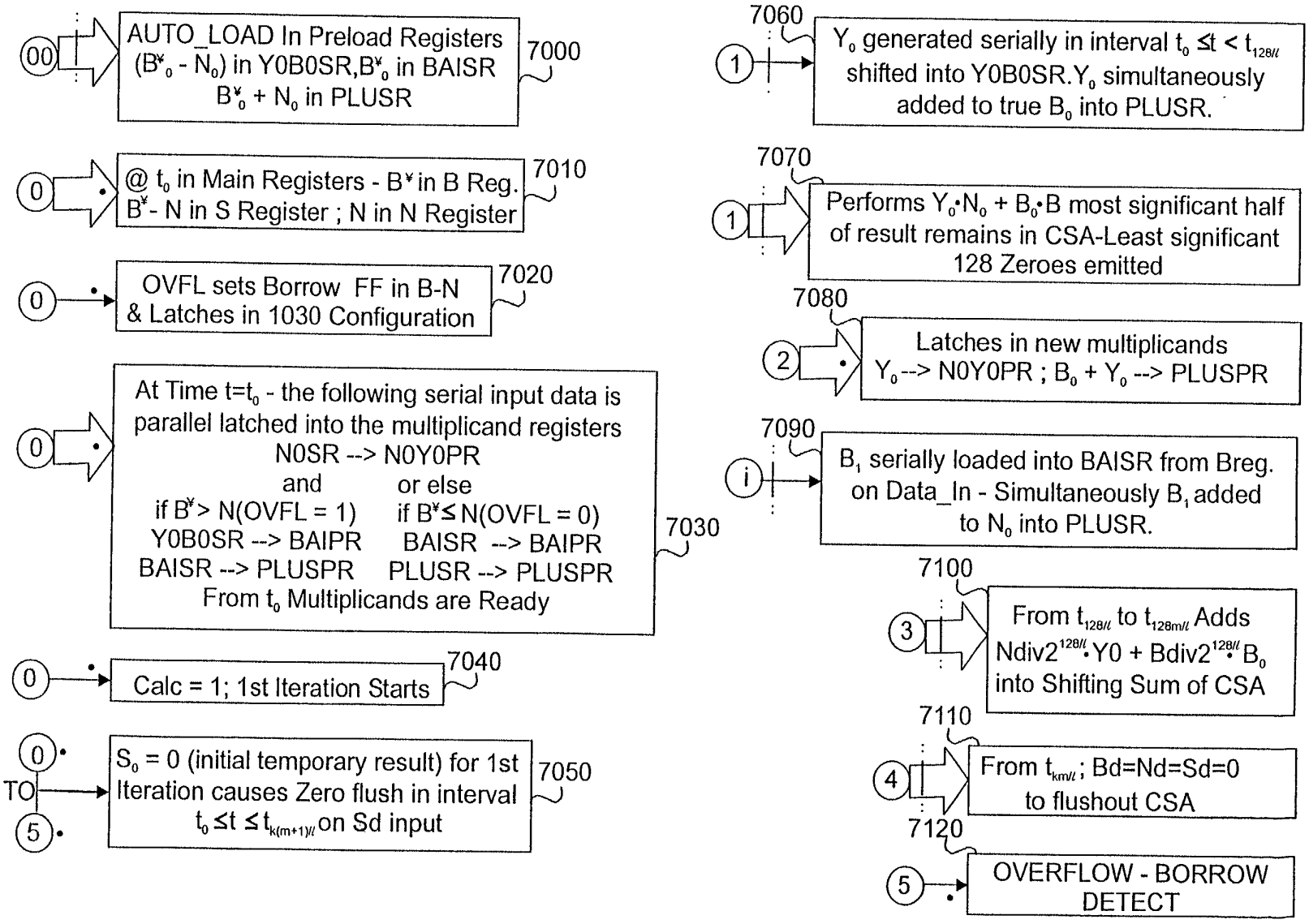

00
AUTO_LOAD In Preload Registers
(B^{*}_0 - N_0) in Y0B0SR,B^{*}_0 in BAISR
B^{*}_0 + N_0 in PLUSR
7000
0
@ t_0 in Main Registers - B^{*} in B Reg.
B^{*} - N in S Register ; N in N Register
7010
0
OVFL sets Borrow FF in B-N
& Latches in 1030 Configuration
7020
0
At Time $t=t_0$ - the following serial input data is parallel latched into the multiplicand registers
N0SR --> N0Y0PR
and
or else
if B^{*} > N(OVFL = 1)
if $B^{*} \leq$ N(OVFL = 0)
Y0B0SR --> BAIPR
BAISR --> BAIPR
BAISR --> PLUSPR
PLUSR --> PLUSPR
From t_0 Multiplicands are Ready
7030
0
Calc = 1; 1st Iteration Starts
7040
0
TO
5
S_0 = 0 (initial temporary result) for 1st Iteration causes Zero flush in interval
$t_0 \leq t \leq t_{k(m+1)/\ell}$ on Sd input
7050
7060
1
Y_0 generated serially in interval $t_0 \leq t < t_{128/\ell}$ shifted into Y0B0SR.Y_0 simultaneously added to true B_0 into PLUSR.
7070
1
Performs $Y_0 \cdot N_0 + B_0 \cdot B$ most significant half of result remains in CSA-Least significant
128 Zeroes emitted
7080
2
Latches in new multiplicands
Y_0 --> N0Y0PR ; $B_0 + Y_0$ --> PLUSPR
7090
i
B_1 serially loaded into BAISR from Breg. on Data_In - Simultaneously B_1 added to N_0 into PLUSR.
7100
3
From $t_{128/\ell}$ to $t_{128m/\ell}$ Adds
$Ndiv2^{128/\ell} \cdot Y0 + Bdiv2^{128/\ell} \cdot B_0$
into Shifting Sum of CSA
7110
4
From $t_{km/\ell}$; Bd=Nd=Sd=0
to flushout CSA
7120
5
OVERFLOW - BORROW DETECT

FIG. 7C

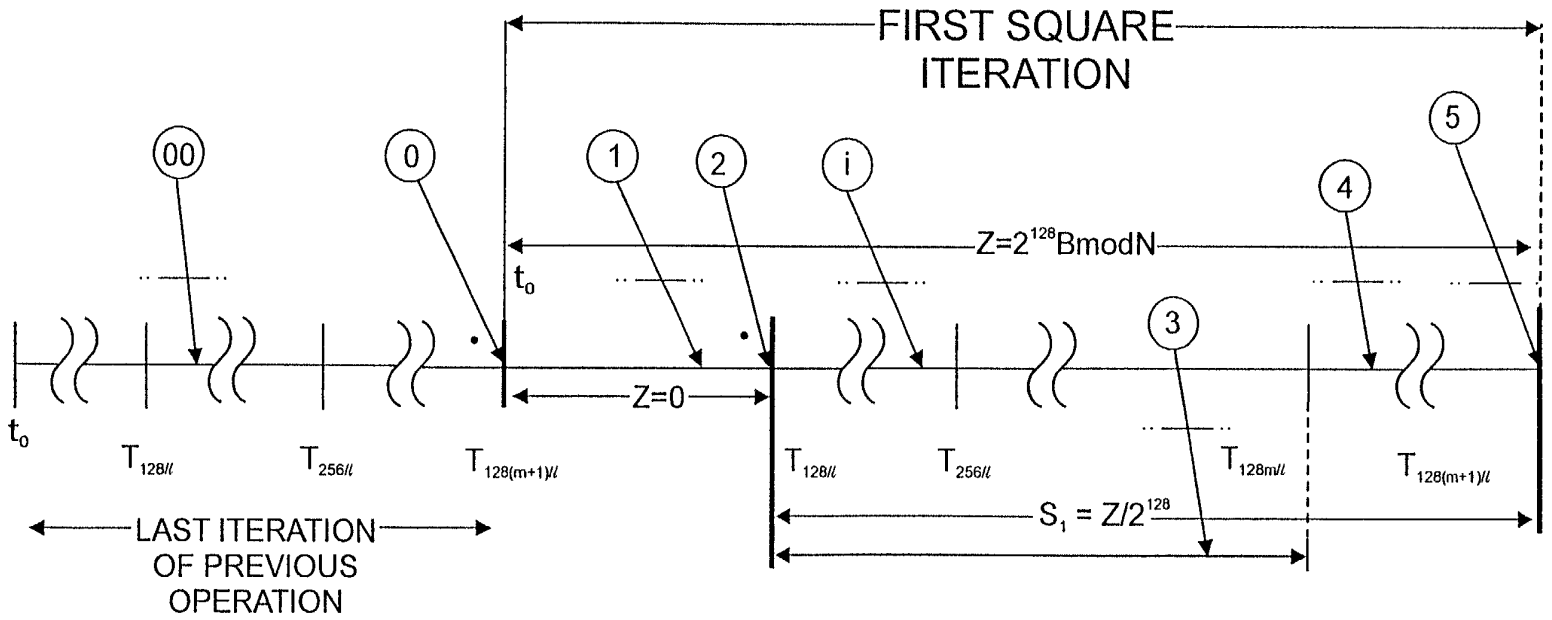

FIRST SQUARE
ITERATION
00
0
1
2
i
3
4
5
Z=2^128BmodN
t0
Z=0
t0
T128/ℓ
T256/ℓ
T128(m+1)/ℓ
T128/ℓ
T256/ℓ
T128m/ℓ
T128(m+1)/ℓ
S1 = Z/2^128
LAST ITERATION
OF PREVIOUS
OPERATION

FIG. 7D

	N_o	N_o^{-1}	$-(N_o^{-1})$
1	0001	0001	1111
3	0011	1011	0101
5	0101	1101	0011
7	0111	0111	1001
9	1001	1001	0111
11	1011	0011	1101
13	1101	0101	1011
15	1111	1111	0001

$\mathcal{S} = 1$
GF(p)
$\ell = 4$

	N_o	$-N_o^{-1} = N_o^{-1}$
1	0001	0001
3	0011	1111
5	0101	0101
7	0111	1011
9	1001	1001
11	1011	0111
13	1101	1101
15	1111	0011

$\mathcal{S} = 0$
No Carry
GF(2^q)
$\ell = 4$

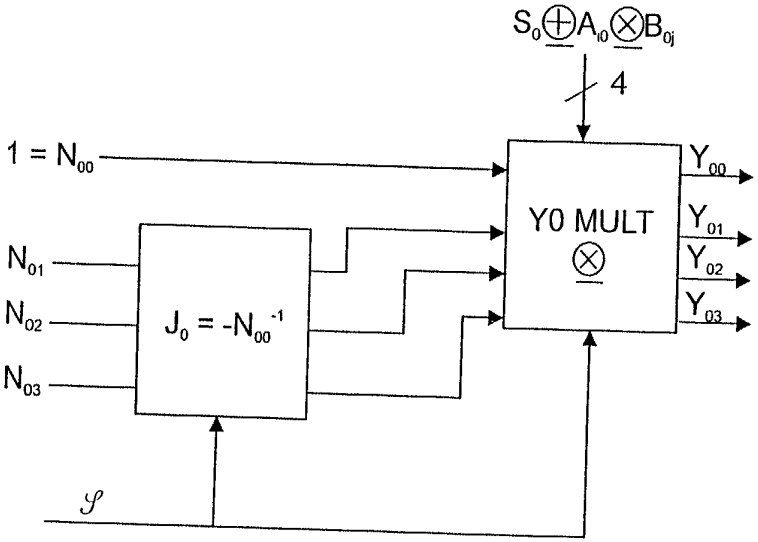
$\mathcal{S} = 1$
GF(p)
$\ell = 2$

N_o	N_o^{-1}	$-N_o^{-1}$
01	01	11
11	11	01

N_o	N_o^{-1}
01	01
11	11

$\mathcal{S} = 0$
No Carry
GF(2^q)
$\ell = 2$

FIG. 8A


$S_0 \underline{\oplus} A_{i0} \underline{\otimes} B_{0j}$
4
$1 = N_{00}$
N_{01}
N_{02}
N_{03}
$J_0 = -N_{00}^{-1}$
Y0 MULT
$\underline{\otimes}$
Y_{00}
Y_{01}
Y_{02}
Y_{03}
$\mathcal{S}$

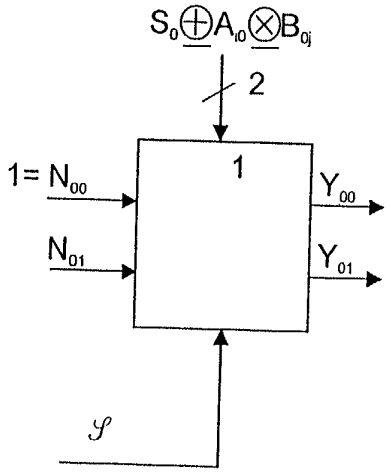

$S_0 \underline{\oplus} A_{i0} \underline{\otimes} B_{0j}$
2
$1 = N_{00}$
N_{01}
1
Y_{00}
Y_{01}
$\mathcal{S}$

FIG. 8B